IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, v. JONATHAN MR. MANZI, Defendant.	))))))))))	Case No. 4:19-CR-3094 **BRIEF IN SUPPORT OF DEFENDANT'S MOTION IN LIMINE TO ADMIT EVIDENCE OF MOTIVE, BIAS, AND CREDIBILITY**

The Defendant, Jonathan Manzi, submits this brief in support of his Defendant's Motion in Eliminate to Admit Evidence of Motive Bias and Credibility.

INTRODCUTION

In this motion, Mr. Manzi seeks to admit evidence that the alleged victim and presumptive star government witness, Troy Pepper, stole proprietary information from Mr. Manzi's company, Ink Labs ("Ink"), shortly before the unlawful access, or "hacking," charged in the Indictment, and held some of the stolen proprietary information in the allegedly-hacked Google account. This evidence is admissible because it goes squarely to Mr. Manzi's motive—or lack thereof—to commit the charged offenses. To prove its felony hacking charges, the government must show that Mr. Manzi hacked Mr. Pepper's Google account and Mr. Pepper's company's Dropbox account "for the purpose of commercial advantage or private financial gain," or that Mr. Manzi "obtained information" worth over $5,000 from each charged offense. *See* 18 U.S.C. § 1030(c)(2)(B). The evidence of Mr. Pepper's prior theft offers an alternative motive: that the alleged hacker may have acted for the purpose of mitigating Mr. Pepper's prior theft and recovering Ink's stolen proprietary data. In addition, evidence of Mr. Pepper's theft is relevant to show the bias and lack of credibility of the alleged victim and linchpin government witness.

FACTUAL BACKGROUND

It is impossible to understand the allegations in this case without understanding the man making the allegations: Troy Pepper. Mr. Pepper is a salesman who worked for Mr. Manzi's chief competitor, Wepa, Inc. ("Wepa"), both before and after working for Mr. Manzi's company, Ink Labs, Inc. ("Ink"). Ink and Wepa are fierce competitors in the market for stand-alone printing kiosks on university campuses. Mr. Pepper worked for Wepa until he was terminated from the company in early 2015. Mr. Pepper then approached Mr. Manzi, who retained Mr. Pepper as a sales consultant for several months in 2015. Ink terminated Mr. Pepper's contract in November 2015 due to spending cutbacks, but Ink renewed his contract in August 2016 as Ink's

sales and revenue grew. Through his work as an Ink salesman, Mr. Pepper became deeply enmeshed in Ink's technology, corporate strategy, and sales and marketing operations.

In February 2017, Mr. Pepper abruptly left Ink and returned to Wepa. Shortly thereafter, Mr. Manzi and others at Ink learned that, in the days leading to his departure, Mr. Pepper accessed Ink's Google drive storage account and viewed and presumably copied a variety of documents containing proprietary Ink information, such as lists of current sales prospects, design schematics, technical specifications for a new product Ink intended to roll out, and various strategic plans and reports. The nature and volume of the proprietary Ink documents Mr. Pepper accessed, combined with the extremely suspicious timing of his access, made it apparent that Mr. Pepper had downloaded sensitive proprietary information for the purpose of using during his imminent employment with Wepa.

A subsequent internal investigation conducted by Ink revealed that Mr. Pepper stole additional proprietary information from Ink by emailing sensitive documents from his Ink email account to his personal Gmail account, both when leaving Ink in February 2017, and when he previously left Ink in November 2015. Ink's internal investigation further revealed that, unbeknownst to Ink, Mr. Pepper had stolen Wepa's proprietary information in early 2015 and attempted to use that information while employed by Ink.

On February 16, 2017, Mr. Manzi, through Ink's outside counsel, sent a cease-and-desist letter to Wepa informing Wepa that Mr. Pepper appeared to have stolen Ink's proprietary information, and demanding that Wepa return or destroy that information and refrain from exploiting it in the future. Wepa responded by generally denying that anything sensitive had been taken but promising not to exploit any of Ink's intellectual property or confidential information.

Ink's counsel sent a similar cease-and-desist letter to Mr. Pepper the next day, who likewise responded by denying the allegations.

It soon became apparent, however, that Wepa was indeed exploiting proprietary information that Mr. Pepper had stolen from Ink. Several of the documents that Mr. Pepper had accessed from Ink's Google drive just before his departure concerned Ink's plans to roll out a miniaturized version of its printing kiosk. The "mini" kiosk was a smart-enabled but scaled-down version of the printing kiosk that was Ink's core product. The advantage of a mini version of the product was that Ink could provide more of those stations and achieve better geographical coverage on college campuses. Ink viewed it as being a substantial advantage in its competition with Wepa.

Just weeks after his departure from Ink, Mr. Pepper began marketing a miniaturized version of a Wepa printing kiosk to prospects he had nurtured while at Ink. One important prospect was the University of Colorado Boulder ("CU Boulder"), which, prior to Mr. Pepper's departure, had expressed exclusive interest in Ink's solution and was contemplating a campus-wide deployment. Ink had spent significant resources developing this relationship from scratch, illuminating how the University would save hundreds of thousands of dollars annually by transitioning to a kiosk-based solution utilizing Ink's miniaturized product. CU Boulder was not evaluating Wepa, which did not have a miniaturized product to satisfy their needs. At the last minute, however, CU Boulder switched its plans, rejecting an anticipated relationship with Ink and instead entering into a contract with Wepa. Ink subsequently learned that Wepa's sales pitch included touting its own, recently-conceived "mini" printing kiosks.

At this point, Mr. Manzi and his team at Ink became extremely concerned that Wepa was continuing to use proprietary information that Mr. Pepper had stolen from Ink. Moreover, Mr.

Manzi and his team were further concerned that they still did not know the extent of the information Mr. Pepper stole or how much of that information he had passed to Wepa. So Ink launched an investigation to determine the extent of Mr. Pepper's theft and how the damage from that theft could be mitigated. It was this defensive investigation that explains why people at Ink might have been interested in accessing Mr. Pepper's Gmail account and Wepa's Dropbox account.

Indeed, the government's own evidence confirms that Mr. Pepper's Google account, which was allegedly hacked, contained a number of proprietary Ink documents. A screenshot of Mr. Pepper's Google drive, which Mr. Pepper provided to the FBI, shows Ink documents related to sales prospects, as well as Ink's agreements with clients. The screenshot shows that Mr. Pepper accessed several of these documents after leaving Ink and rejoining WEPA. In addition, the screenshot indicates that at least one of the documents accessed on July 2, 2017, during the hack allegedly committed by Mr. Manzi, was a document that Mr. Pepper had stolen from Ink (entitled, "Agreement Form tpepper@inkcloud.me Ink Labs Inc. – Mail Files). This evidence further demonstrates that any alleged hack was likely motivated by a desire to protect Ink from Mr. Pepper's theft and not to steal Wepa's data or obtain a commercial advantage or private financial gain.

The defense expects it could prove the facts summarized in the prior section through a relatively small number of documents, as well as brief testimony explaining the significance of said documents. This would include the following categories of documents:

- Emails containing proprietary Ink information that Mr. Pepper forwarded from his Ink email account to his personal Google account (i.e., the account referenced in the Indictment) prior to his departures from Ink;
- Snapshots of Ink's Google drive taken shortly after Mr. Pepper's departure from Ink showing that Mr. Pepper accessed dozens of documents containing Ink

proprietary data the week before leaving Ink for WEPA, as well as the documents themselves, if necessary for context;

- Internal Ink emails from Mr. Manzi and others between February and June 2017 expressing concern about Mr. Pepper's theft of Ink proprietary information and WEPA's exploitation thereof; and
- Cease-and-desist letters sent in February 2017 from Ink's outside counsel to Mr. Pepper and WEPA documenting Ink's concerns about Mr. Pepper's theft of proprietary information and WEPA's exploitation thereof.

The defense expects to call a few witnesses to explain the significance of these documents. Those witnesses may include Mr. Manzi himself, employees of Ink who were involved in the events in question, and an expert witness who could provide a brief explanation of the Google drive evidence referenced above for the benefit of less tech-savvy jurors.

ARGUMENT

I. EVIDENCE OF MR. PEPPER'S THEFT IS RELEVANT TO SHOW THE MOTIVE AND INTENT BEHIND THE ALLEGED HACKS AND REBUT THE GOVERNMENT'S EVIDENCE OF MOTIVE AND INTENT.

Evidence that Mr. Pepper, the alleged victim, stole proprietary information from Ink and appears to have passed the stolen data to Wepa, the other alleged victim, and stored it on one of the allegedly-hacked accounts, is highly relevant to Mr. Manzi's motive—or lack thereof—to commit the charged crimes. As multiple courts have held, "'motive is always relevant in a criminal case, even if it is not an element of the crime.'" *United States v. Hill*, 643 F.3d 807, 843 (11th Cir. 2011) (quoting *United States v. Sriyuth*, 98 F.3d 739, 747 n.12 (3d Cir. 1996)); *see also United States v. Day*, 591 F.2d 861, 874-75 (D.C. Cir. 1978) ("Motive is always relevant." (quoting 1 Wigmore on Evidence § 118 at 558, 561 (3d ed. 1940))).

The Eighth Circuit has frequently held that motive evidence is relevant and admissible to prove the defendant did or did not have the requisite *mens rea*. *See United States v. Felix*, 867 F.2d 1068, 1072 (8th Cir. 1989) (noting that, "[w]here specific intent and guilty knowledge are

elements of the crime charged," courts frequently admit prior bad acts "to establish intent or motive to commit the crime charged"); *Morris v. Union Pac. R.R.*, 373 F.3d 896, 901 (8th Cir. 2004) (noting that, because "[i]ntent rarely is proved by direct evidence, . . . a district court has substantial leeway to determine intent through consideration of circumstantial evidence, witness credibility, [and] motives of the witnesses in a particular case"). And just as the government can offer evidence of motive, the defense may respond with motive evidence of its own. *See Achterberg v. Albaugh, LLC*, No. 5:16-CV-06097-DGK, 2017 U.S. Dist. LEXIS 197291, at *2 (W.D. Mo. Nov. 30, 2017) (admitting evidence of defendant's "good" motives in an employment discrimination case "to rebut Plaintiff's allegation that it had an improper motive or intent when it terminated Plaintiff"). In addition, motive evidence is frequently relevant to proving or disproving a crime's actus reus because "[m]otive is a state of mind . . . showing the probability of appropriate ensuing action." *Day*, 591 F.2d at 874-75 (quotations omitted); *United States v. Sanford Ltd.*, 878 F. Supp. 2d 137, 145 (D.D.C. 2012) ("Although Sanford is correct that monetary proceeds are not an element of any offense charged, the government has demonstrated that at least some evidence of monetary proceeds will be relevant because it is probative of the incentives and priorities of the defendants and, thus, will have a tendency to make it more or less probable that the defendants committed the charged offenses.").

Here, the government has alleged, as necessary elements of the charged felonies, that the computer intrusions were "committed for purposes of commercial advantage or private financial gain" and that "the value of the information obtained [from the charged computer intrusions] exceeds $5,000." 18 U.S.C. § 1030(c)(2)(b)(i) & (iii). The defense's proposed motive evidence helps rebut the required *mens rea* because it suggests that any hacking that occurred could have

been done to retrieve stolen property and mitigate the harm from Mr. Pepper's theft, not "for the purpose of commercial advantage or private financial gain." The proffered motive evidence also rebuts the alleged *actus reus* of obtaining information worth over $5000. Indeed, if the alleged hackers were motivated by a desire to mitigate the harm from Mr. Pepper's theft, it becomes far less likely that they changed course and stole $5,000 worth of unrelated proprietary information from Wepa, as the government appears to allege.

A. Evidence of Mr. Pepper's Theft, and Mr. Manzi's Knowledge Thereof, Is Relevant to Show that Mr. Manzi Did Not Act for Commercial Advantage or Private Financial Gain.

The Computer Fraud and Abuse Act (CFAA) is an extremely broad statute, making it a crime, *inter alia*, "to intentionally accesses a computer without authorization . . . and thereby obtain[] . . . information." 18 U.S.C. § 1030(a)(2). CFAA violations are, by default, misdemeanors. *See* Orin Kerr, COMPUTER CRIME LAW, 88 (West 4th Ed. 2017) (1030(a)(2) violations ordinarily are misdemeanors); *Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (noting that §1030(a)(2) violations give rise to misdemeanor and civil liability, as well as felony liability where there are aggravating circumstances). Section 1030(a)(2) violations only become felonies where the government proves, beyond a reasonable doubt, one of the aggravating circumstances specified in § 1030(c)(2)(B).

One of the aggravating circumstances alleged in this case is that "the offense was committed for purposes of commercial advantage or private financial gain." 18 U.S.C. § 1030(c)(2)(B)(i). The CFAA does not define the term "for purposes of commercial advantage or private financial gain," and there do not appear to be any published cases interpreting the phrase as used in the CFAA. The phrase is used in several other criminal statutes, however, and in those contexts, courts have interpreted the phrase to require that the defendant seek some

advantage above and beyond his "financial status quo." *See, e.g.*, *United States v. Garcia*, 883 F.3d 570, 574 (5th Cir. 2018).

In *Garcia*, the Fifth Circuit interpreted the Human Smuggling Statute, which, like the CFAA, provides for increased punishment if the offense is committed "for the purpose of commercial advantage or private financial gain." 8 U.S.C. § 1324(a)(1)(B)(1). The defendant argued that, because he only intended to obtain reimbursement for the costs of the smuggling he committed, he did not act "for the purpose of commercial advantage or private financial gain." The Fifth Circuit held that this was indeed a defense, holding that "the Government must prove an anticipated gain beyond that of a pure reimbursement" because "[a] smuggler who seeks only her incurred smuggling costs seeks no economic benefit at all—she simply aims to maintain her financial status quo of zero dollars spent." *Garcia*, 883 F.3d at 574. Interpreting the same statute, the Eleventh Circuit similarly held that acting "for the purpose of commercial advantage or private financial gain" requires a motive to seek profit, not merely compensation. *See United States v. Chang Qin Zheng*, 306 F.3d 1080, 1086 (11th Cir. 2002) (holding that the "common-sense understanding of 'commercial advantage' is a *profit* or gain in money obtained through business activity" and "the common meaning attributed to 'private financial gain' is an *additional profit* specifically for a particular person or group") (emphasis added).

Courts have reached the same conclusion when interpreting "commercial advantage or private financial gain" as used in 47 U.S.C. § 553(c)(3)(B). Section 553(c) allows cable companies to sue those who gain unauthorized access to their services, and subsection (c)(3)(B) authorizes punitive damages when the offense is committed "for the purpose of commercial advantage or private financial gain." Courts have held that the phrase requires more than a desire to avoid the cost of paying for cable, reasoning that "[a] finding that avoidance of the costs

associated with premium services is a 'private financial gain' would necessitate such a finding in virtually every cable piracy case." *Comcast of S. New Eng., Inc. v. Kacavas*, Civil Action No. 07CV10780-NG, 2007 U.S. Dist. LEXIS 93655, at *11 (D. Mass. Dec. 18, 2007). Instead, "the clause should be read as providing for increased damages in the limited circumstance that the defendant *reaps some form of profit* from the unauthorized reception." *Id.* at 12 (emphasis added); *see also Comcast Cable Commc'ns v. Adubato*, 367 F. Supp. 2d 684, 693 (D.N.J. 2005) (holding that to qualify as commercial advantage or private financial gain, the defendant must have used the device "to further some commercial venture or profited in some way from the device beyond simply . . . using the illegal device to watch programs for which payment should have been made"); *American Cablevision of Queens v. McGinn*, 817 F. Supp. 317, 320 (E.D.N.Y. 1993) (holding that "private financial gain" should not be read to encompass defendant's "gain" from receiving broadcasts himself: such an interpretation would render "gain" enhancement superfluous because all violations would result in gain). As particularly relevant here, those courts have reasoned that "although they might be economically equivalent, reaping a 'financial gain' and avoiding a payment are different in ordinary meaning, and the statute should not be presumed to conflate them." *Kacavas*, 2007 U.S. Dist. LEXIS 93655, at *10-*11.

Following the cases above, this Court should find that acting "for the purpose of commercial advantage or private financial gain" requires that the defendant seek some "profit" beyond his "financial status quo." *Garcia*, 883 F.3d at 574. Such a profit-seeking motive is absent if the defendant merely acts to reclaim his own property and mitigate the harm caused by a theft. In common parlance, such a person seeks to avoid an unjust loss, not "reap[] a 'financial gain.'" *Kacavas*, 2007 U.S. Dist. LEXIS 93655, at *11.

By analogy, a person who enters another's home intending only to reclaim their own property is guilty of a trespass, but not a burglary because she did not have "the specific intent to commit the crime of theft." *Auman v. People*, 109 P.3d 647, 663 (Colo. 2005) (reversing burglary conviction where jury instructions permitted the jury to convict a woman who trespassed in her ex-boyfriend's home for the purpose of reclaiming her own property). Similarly, a person who accesses a computer without authorization for the purpose of reclaiming his own property, or that of his or her company, is guilty of misdemeanor computer trespass but not felony computer burglary because the trespass was not "for the purpose of commercial advantage or private financial gain." 18 U.S.C. § 1030(c)(2)(B)(1).[1]

Accordingly, evidence that one alleged victim, Mr. Pepper, stole proprietary information from Ink, held it in the allegedly-hacked Google account, and likely passed it to Wepa, the other alleged victim, and that the alleged hacker was aware of this prior to the alleged hacking, is highly relevant to that hacker's possible motive. In particular, these facts give rise to a possible motive of reclaiming Ink's own property and thus directly rebuts an essential element of all four counts charged in the indictment, i.e., that the alleged hacker acted "for commercial advantage or private financial gain."

---

[1] To the extent there is any doubt about whether a person who merely seeks to reclaim their own property acts "for the purpose of commercial advantage or private financial gain," the Rule of Lenity requires that doubt be resolved in favor of the defendant. *See United States v. Davis*, 139 S. Ct. 2319, 2333 (2019) ("the rule of lenity[] teach[es] that ambiguities about the breadth of a criminal statute should be resolved in the defendant's favor. That rule is perhaps not much less old than the task of statutory construction itself.") (internal quotations omitted).

B. Evidence of Mr. Pepper's Theft, and Mr. Manzi's Knowledge Thereof, Is Relevant to Rebut the Government's Allegation that Mr. Manzi Stole WEPA's Proprietary Information During the Alleged Hacks.

The motive evidence discussed above is also relevant to rebutting another essential element of all four charged crimes: that "the value of the information obtained [from each intrusion] exceeds $5,000." 18 U.S.C. § 1030(c)(2)(B)(iii). Evidence that Mr. Manzi and his team at Ink may have been motivated not by any desire to steal proprietary information from Wepa, but simply by a desire to reclaim proprietary information stolen from Ink, undermines the government's theory that Mr. Manzi "obtained" over $5000 worth of information during the hack. Indeed, there is a strong argument that one does not "obtain" $5000 worth of information if he is only viewing and/or deleting copies of his or his company's own information that he already possesses.

Motive evidence is especially relevant in this case because of the dearth of direct, forensic evidence showing what information was exfiltrated from the allegedly-hacked accounts. The government appears to be relying on the inference that Mr. Manzi must have stolen Wepa's proprietary information during the hacks because why else would someone hack Wepa? If the jury believes the alternative motive of reclaiming proprietary data, however, that will make it more likely that the scope of information obtained during the hacks matched that narrower motivation. *See Day*, 591 F.2d at 874-75 ("Motive is a state of mind . . . showing the probability of appropriate ensuing action...") (internal quotations omitted). By analogy, one might infer that someone who breaks into a house intended to and did steal valuable property from the house, since stealing property is the most natural motivation for such a break-in. But that inference is called into question when one learns that the trespasser was an ex-girlfriend of the victim whose property was inside the home. *See, e.g.*, *Auman*, 109 P.3d at 663. In the same way, evidence that the alleged victim in this case had previously stolen proprietary information from Mr.

Manzi's company, and held such information in at least one of the allegedly-hacked accounts, provides an alternative motive that weakens the inference that Mr. Manzi must have stolen $5000 worth of information belonging to WEPA.

II. EVIDENCE OF MR. PEPPER'S THEFT IS RELEVANT TO SHOW THE CREDIBILITY AND POTENTIAL BIAS OF THE ALLEGED VICTIM AND PRESUMPTIVE STAR GOVERNMENT WITNESS.

Evidence of Mr. Pepper's theft of Ink's proprietary information is also relevant to show the credibility and bias of the alleged victim and the presumptive star government witness. As the Eighth Circuit has repeatedly held, "the bias of a witness is always relevant." *United States v. Caldwell*, 88 F.3d 522, 525 (8th Cir. 1996); *see also United States v. Abel*, 469 U.S. 45, 52 (1984) ("Proof of bias is almost always relevant because the jury, as finder of fact and weigher of credibility, has historically been entitled to assess all evidence which might bear on the accuracy and truth of a witness' testimony."); *United States v. Drapeau*, 414 F.3d 869, 880-81 (8th Cir. 2005) ("It was an error of law and therefore an abuse of discretion for the district court to conclude that the bias and motives of the government's key witness did not mean anything."); *Johnson v. Brewer*, 521 F.2d 556, 562 n.13 (8th Cir. 1975) ("In courtroom parlance, facts showing bias are not collateral.") (internal quotations omitted).

In addition, evidence of an alleged victim's pertinent character trait is relevant and admissible, whether the alleged victim testifies or not. *See* Fed. R. Evid. 404(a)(2)(B) ("[S]ubject to the limitations in Rule 412, a defendant may offer evidence of an alleged victim's pertinent trait . . ."); *see also id.* Comm. Note on 2006 Amend. ("In criminal cases, the so-called 'mercy rule' permits a criminal defendant to introduce evidence of pertinent character traits of . . . the victim . . . because the accused, whose liberty is at stake, may need a counterweight against the strong investigative and prosecutorial resources of the government.") (quotations omitted).

Here, evidence that Mr. Pepper stole proprietary information from Mr. Manzi's company is relevant to his character for truthfulness, credibility, and potential bias. As an initial matter, such evidence shows Mr. Pepper's poor character for truthfulness and bias against Ink and Mr. Manzi generally. More specifically, evidence of Mr. Pepper's theft is especially relevant in this case because it appears that the government is largely relying on Mr. Pepper's search of his own Google account for its evidence of what information Mr. Manzi allegedly stole (the government has not, for instance, produced logs from Google showing what information was accessed during the alleged intrusion). But Mr. Pepper has an obvious incentive to steer the FBI aware from any evidence indicating that the hack targeted information that Mr. Pepper himself previously stole from Ink. Mr. Pepper's incentive was to provide the FBI with supposed evidence that the hack targeted Wepa information that Mr. Pepper lawfully possessed. Thus, because the government will rely on evidence produced by Mr. Pepper, evidence of Mr. Pepper's credibility and bias is relevant whether he testifies or not.

CONCLUSION

For forgoing reasons, Mr. Mr. Manzi respectfully requests that the Court admit the evidence summarized above as relevant to the alleged perpetrator's possible motive, and to the credibility and potential bias of the alleged victim and presumptive star government witness.

THE WEINHARDT LAW FIRM

/s/ Mark E. Weinhardt
Mark E. Weinhardt AT0008280
2600 Grand Avenue, Suite 450
Des Moines, IA 50312
(515) 244-3100
mweinhardt@weinhardtlaw.com

and

BERRY LAW FIRM
Justin B. Kalemkiarian, #25415
6940 O Street, Suite 400
Lincoln, NE 68510
justin@jsberrylaw.com
(402) 466-8444

ATTORNEYS FOR JONATHAN MR. MANZI

CERTIFICATE OF SERVICE

I hereby certify I have caused this document to be filed with the Clerk of the United States District Clerk, District of Nebraska, using the CM/ECF system which sent notification to the government, on January 28, 2022.

/s/ Mark E. Weinhardt
Mark E. Weinhardt, AT0008280